AOIT Computer Systems

Lesson 4

Malware

Student Resources

|  |  |
| --- | --- |
| Resource | Description |
| Student Resource 4.1 | Anticipation Guide: Computer Malware |
| Student Resource 4.2 | Reading: How Malware Works |
| Student Resource 4.3 | Worksheet: Compare and Contrast Malware Chart |
| Student Resource 4.4 | Assignment: Name That Malware PowerPoint Presentation |

Student Resource 4.1

Anticipation Guide: Computer Malware

Student Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:\_\_\_\_\_\_\_\_\_\_\_

Directions: For each of the statements below, underline “I agree” if you think the statement is accurate or “I disagree” if you disagree with it. Write one reason to explain your guess.

|  |  |
| --- | --- |
| All computer viruses need user interaction to help them spread. | |
| My guess: | I agree I disagree |
| My reason: |  |
| I learned: |  |
| Websites need your permission to take personal information from your computer. | |
| My guess: | I agree I disagree |
| My reason: |  |
| I learned: |  |
| The only way to protect yourself against malware is to purchase a special piece of software to prevent it. | |
| My guess: | I agree I disagree |
| My reason: |  |
| I learned: |  |
| As long as you recognize who an email is from, it is safe to open something that person sends you. | |
| My guess: | I agree I disagree |
| My reason: |  |
| I learned: |  |

Student Resource 4.2

Reading: How Malware Works

Malware at Work

Malicious software, or *malware*, refers to any unwanted program that serves to do harm and is transmitted to your computer without you knowing it. Malware includes computer viruses, worms, Trojan horses, spyware, adware, rootkits, phishing, and fake antiviruses. Some of the signs your system is infected with malware include receiving more pop-up ads than usual, your system working slower than it used to, programs taking longer to load, your system having less memory available than usual, or experiencing strange or bizarre error messages, graphics, or sounds. It is also possible to have no symptoms from the infection as it works quietly in the background. There are many different types of malware. The following are some of the more common ones.

Computer Viruses

A *virus* is a computer program that has been specially designed to infect files on a single computer. It spreads by attaching itself to a file that, when opened, copies the virus to other files on the computer. The virus can spread when users share infected files with other computers. Viruses cause a wide array of problems. Sometimes they cause only mildly annoying effects, such as displaying bugs crawling around on your screen. Other times they can cause major damage, such as erasing everything on your hard drive. Sometimes viruses are so hidden that you don’t even know you have them running on your system.

Antivirus programs, such as Symantec’s, McAfee’s, and Mircrosoft’s Security Essentials protect your system by searching for viruses’ *signatures* (their characteristic byte patterns) and guarding against those viruses.

Typical signatures of many types of malware include their ability to start themselves and prevent detection. Some viruses can change their names, mask a difference in file size (a virus attaching itself to another file increases the size of that file), and transform themselves to remove the characteristics that antivirus programs typically look for. Antivirus companies update their products often and offer those updates to subscribers, but virus makers take advantage of many people who don’t update their antivirus programs.

Worms

A *worm* is a self-replicating computer code that is designed to spread from one computer to another. A worm makes copies of itself through a network without using a host file or user intervention. It automatically scans the network for vulnerable systems and copies itself to those systems very quickly. This process causes problems by overloading network and hard drive space rather than by performing a specific damaging act like viruses do.

Once delivered, a worm can spread itself by sending copies to everyone in a person’s email address book, and then everyone in their address book, on down the line. One worm can infect thousands of computers and networks. Many worms are designed only to spread, but other worms can deliver “payloads”—code designed to be delivered to an unsuspecting system. Payloads can be designed to delete files or automatically send infected files (viruses) by email. A common payload for worms is to install a backdoor on the infected computer. These backdoors can then be exploited by other malware or spam senders.

Worms generally spread by using vulnerabilities (or weaknesses) in operating systems and can usually be prevented by keeping your operating system up-to-date, installing antivirus software, and setting up a firewall. Users also need to be careful about opening unexpected emails or attachments and should avoid visiting any sites linked to in emails.

Spyware

*Spyware* installs itself on your computer to collect personal information from you and sends it over the Internet to users who intend to use the information for harm. It is usually hidden from the user and is difficult to detect. Sometimes the information is collected by keylogger programs, which record your keystrokes. It is difficult to know whether a computer is infested with spyware, but sometimes spyware is the cause of pop-up ads appearing whenever you’re connected to the Internet, or sometimes your home page will keep changing to a page you don’t want.

Spyware is typically hidden in email attachments, freeware or shareware, instant messaging programs, or malicious websites (offshore or foreign websites can be notorious sources of spyware). You can catch spyware simply by clicking a link that leads to one of these sites.

Users can detect, quarantine, and remove spyware on their systems by using any one of a number of free and subscription-based antispyware software programs available, including Microsoft Security Essentials, Norton AntiVirus, McAfee VirusScan Plus, Spybot: Search & Destroy, Ad-Aware, Webroot Spy Sweeper, Spyware Doctor, Stopzilla, and SpySubtract. Many antivirus programs can catch multiple types of threats; they typically include tools that scan for and remove spyware from your system. You can set these types of programs to scan your computer in real time (while you’re using your computer) or at certain times during the day. But often it helps simply to be cautious and not visit websites or download programs if you’re not sure about the source of them. Common sense is often the first and best defense against spyware.

A specific piece of software that is used to deliver spyware or viruses is called a *Trojan horse* or *Trojan*. It was named after a famous Greek myth that tells the story of 3,000 warriors hiding inside a huge wooden horse to get inside the gates of a town called Troy. The Greek wooden horse appeared to be a gift to the town of Troy, but it actually was an act of war. A computer Trojan is a piece of software that appears to do one thing but actually does another. Computer-based Trojan horses are destructive and can do any of the following:

* Remote-access Trojans allow others access into your computer.
* Data-sending Trojans are very dangerous. They look for text, logins, and passwords to enable others to steal a user’s identity.
* Destructive Trojans work at destroying data.
* Proxy Trojans turn your computer into a remote workstation (which is then called a *zombie*). Spammers then use your computer as a base of operations to send out spam.
* FTP Trojans open a port on your computer to enable remote access.
* Security software disabler Trojans prevent your antivirus or antispyware programs from working properly.
* Denial-of-service (DoS) attack Trojans send out useless information to a targeted site, slowing down or even disabling that site.

Adware

Technically, advertising-supported software, or *adware*, refers to any software that automatically plays, displays, or downloads advertisements to you. Some programs, such as Gmail, Facebook, and LinkedIn, present advertisements instead of charging for the software. In this way, adware is like television commercials that pay for programs so that people can watch an episode of their favorite show. Most adware, however, is actually a type of spyware that presents advertisements to you based on what it has learned about you from your web surfing habits and any information you might give online. But it is illegal for someone to access information from your computer without your permission. The trick both adware and spyware makers often use to get your permission is to make you click Accept to some lengthy end user license agreement (EULA) that’s written by lawyers and is very difficult for others to understand. It’s very easy to give adware companies permission to access your web surfing habits and personal data without realizing it. Even so, adware is generally considered less damaging than spyware. Sometimes, instead of being called *malware*, adware is called *grayware*, because it’s more of an annoyance than a danger.

If you want to prevent the installation of adware on your system, many of the same programs that scan for and remove spyware will also remove adware. You can also set your Internet browser to not accept cookies (which are files that some websites copy to your computer so that they can remember who you are).

Rootkits

Unlike viruses and worms that attempt to spread to other systems, a *rootkit* usually limits itself to maintaining control of one system. Some rootkits load before your computer is fully booted (started up), so antivirus programs can miss them. Sometimes you can find out whether you have a rootkit on your system by starting your computer in Safe Mode (while the computer is booting, press F8) and running your antivirus software from there. Rootkit removal can be complicated at best or practically impossible, especially when the rootkit resides in the kernel or core files of the operating system. Your time might be better spent re-installing your operating system or completely re-imaging your computer instead of attempting to find and omit all the components of a rootkit.

Rootkits can take total control over your computer and hide your Windows utilities (like Task Manager), hide new network connections, and disable programs that a system administrator would use to detect special privileged access to the computer. Rootkits are introduced to your system when you install another piece of software. Some rootkits are intended for good purposes, such as restoring an offsite computer, but they can also easily be misused.

The best way to prevent a rootkit infection is to be very careful about which software you install. There are many free rootkit scanners/removers available, including Sophos Anti-Rootkit, RootRepeal, F-Secure BlackLight Rootkit Eliminator, and RootkitRevealer.

Spam

Technically, *spamming* is misusing any electronic messaging system to send unwanted messages. Instant messaging, web search engines, blogs, mobile phones and mobile phone messaging, and Internet forums, are just some of the targets of spammers. The most famous and widely recognized form of spam is email spam. Email spam is usually used to advertise something or to attempt to cheat people out of money. But more and more often, spam is being sent to deliver viruses that will be activated if a user opens an attachment or follows a link to an infected advertised site.

Email spam can be sent via “zombie networks,” which are networks of virus- or worm-infected personal computers around the world. These infections can install backdoors (ways into a program that avoid its usual login procedure) that a spammer can use to take control over another computer. Sometimes spam even makes it look as if the innocent person who owns the zombie computer is sending the email instead of the spammer. That’s why it’s important to make sure you don’t open any strange attachments, even from friends. It is often very hard to tell where spam originates.

Most email programs have filters to help people eliminate or at least reduce the amount of spam that arrives in email, but a simple solution is to just be careful about what email attachments you choose to open. It is also very important to avoid giving your email address to unknown recipients.

Phishing

Phishing is an attempt to acquire private information by sending a user an email or message masquerading as something sent by a known and trusted institution; for example, the email may look like it is coming from the user’s bank. The user is usually asked to provide user IDs, passwords, or credit card information on a website that looks like the institution’s real site. Those perpetrating the fraud use any information supplied by the user to steal money by transferring funds from the user’s account.

Legitimate institutions do not ask for such information in a message or an email. To avoid being a victim of phishing, do not respond to requests for information unless you completely verify that the request is legitimate (by phoning the bank, for example).

Fake Antiviruses

Fake antiviruses (or rogueware) are an Internet fraud using computer malware that tries to fool the user into buying fake antivirus software. The fraud occurs when the user visits a website for information and clicks. A pop-up displays that looks like a legitimate antivirus warning, informing the user he has a virus and locking the system so the user cannot move to another window. The pop-up message asks the user to buy and install software that will purportedly remove the fake virus. In some cases, when you click, a Trojan horse virus is installed on your machine that produces even more fake antivirus messages.

To avoid being the victim of such a fraud, never click on an antivirus warning pop-up unless you are absolutely sure the message is from trusted antivirus software that you have already installed on your machine.

Student Resource 4.3

Worksheet: Compare and Contrast Malware Chart

Student Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:\_\_\_\_\_\_\_\_\_\_\_

Directions: During the class discussion, take notes in the boxes on this chart. You will need this information to help you prepare your PowerPoint presentation.

|  |  |  |
| --- | --- | --- |
|  | How is it caught? How does it spread? | What does it do? |
| Virus |  |  |
| Worm |  |  |
| Spyware |  |  |
| Adware |  |  |
| Rootkit |  |  |
| Spam |  |  |
| Phishing |  |  |
| Fake Antivirus |  |  |

Student Resource 4.4

Assignment: Name That Malware PowerPoint Presentation

Directions: Work on the Internet to find the following information about the famous malware your group has been assigned. Collect the information, and then use it to fill in the PowerPoint template your teacher provides you. You will then present your finished PowerPoint presentation to your class.

Your presentation should include the following points:

* Your malware’s name
* The type of malware that describes your sample
* How it spreads
* What it does
* The best ways to prevent it
* The best ways to cure it
* Additional interesting facts about your malware

You must consult and cite a minimum of three Internet sources to prepare your PowerPoint presentation.

Resources

The following online resources may be useful in your research. Remember to consult other websites as well by searching for terms associated with your malware example.

* Symantec Antivirus and Security Software  
  <http://www.symantec.com>
* McAfee Software and Intrusion Prevention Solutions  
  <http://www.mcafee.com>

Check to make sure your assignment meets or exceeds the following assessment criteria:

* The presentation identifies the correct type of malware.
* The presentation correctly describes what the malware does.
* The presentation describes the best ways to prevent and/or cure the problems.
* The notes for the presentation provide accurate descriptions.
* The oral presentation is clear and uses the material in the notes to enhance what the viewers see on the slides.
* The PowerPoint is neat and uses proper spelling and grammar.